Paper Title:
Predict And Prevent DDOS Attacks Using Machine Learning and Statistical Algorithms

Large Scale Paper Link:
https://cs.paperswithcode.com/paper/predict-and-prevent-ddos-attacks-using

****1.1 Motivation/purpose/aims/hypothesis:****

Distributed Denial of Service attacks are a type of cybercrime attack that aims to take down websites and online applications by overwhelming them with network traffic. A network of compromised computers or botnets is used to carry out these sorts of attacks. The paper discusses different types of DDoS attacks such as UDP floods, ICMP floods, etc. The author aims to resolve these sort of attacks using machine learning. The goal of this paper is to find the best algorithms to separate DDoS aatacks from regular traffic and train their model to identify the attacks in order to prevent them.

****1.2 Contribution:****

The study proposes a DDoS attack detection system using machine learning. The system combines seven different classifiers such as naive Bayes, KNN, logistic regression, CNN, XGboost, AdaBoost, and random forest to achieve high accuracy with low false positives. Each classifier analyzes the dataset CICDDoS2019 and its features and makes its own prediction. The final output is a combined decision based on the accuracy, precision, and recall of all the individual classifiers.

****1.3 Methodology:****

In this study, the authors have used machine learning models relating to DDoS attack detection. The CICDDoS2019 dataset has been used to test their model. Firstly, the data is merged and relevant features are selected in order to preprocess the data. The dataset is a collection of network traffic data that includes both normal and denial-of-service network flows. As expected, the dataset is imbalanced having more attack traffic than normal traffic in order to train the model properly. The authors have used a technique called SMOTE to oversample the normal traffic in the dataset. As a result, a balanced dataset was produced which had roughly 50% normal traffic and 50% attack traffic.

****1.4 Conclusion:****

DDoS is a major problem for online services. For large networks, this sort of attack might halt their services resulting in huge losses. The authors propose using machine learning to predict and prevent these attacks. They found that XGBoost is the best algorithm for this task and that five specific features are important for prediction. The author further acknowledges that they will

keep improving their model and algorithms to keep looking for the best solution for this sort of attacks.

****Limitations****

****2.1 First Limitation/Critique:****

There can be a lot of ways DDoS attacks can be carried out the model is only limited to the features that are included in the dataset. If there are variations of attacks that are not included in the dataset, then the model won't be able to detect and sort of DDoS attack.

****2.2 Second Limitation/Critique:****

This DDoS detection model is trained on a single dataset CICDDoS2019. Real-world attack variations might not be fully captured in this dataset, potentially affecting the generalizability of the model.